CODEC NET

Security Operations Center

Monthly Report

Global Finance Corp

Executive Summary

Report Period: September 25, 2025 - October 25, 2025

Top 10 Security Alerts

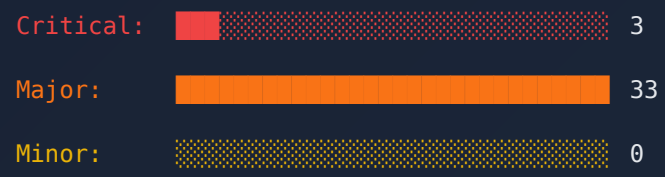
#	Severity	Alert Description	Host/Agent	Count	Last Seen
1	Major	Possible kernel level rootkit	wazuh-VMware-Virtual-Platform	4	10/03/25 9:04 PM
2	Major	Auditd: Process ended abnormally.	Yara_New_2.0	4	09/29/25 5:21 PM
3	Major	New user added to the system.	Yara_Final	3	09/29/25 4:57 PM
4	Critical	File "/root/testfile.txt" is a positive match. Yara rule: Test_Yara	Yara_New_2.0	2	09/29/25 5:24 PM
5	Major	New group added to the system.	Yara_Final	2	09/29/25 4:57 PM
6	Major	SCA summary: CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Score less than 30% (26)	windows	2	09/26/25 5:04 PM
7	Major	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure sshd UsePAM is enabled.: Status changed from passed to failed	wazuh-VMware-Virtual-Platform	1	10/03/25 9:43 PM
8	Major	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure sshd PermitUserEnvironment is disabled.: Status changed from passed to failed	wazuh-VMware-Virtual-Platform	1	10/03/25 9:43 PM
9	Major	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure sshd PermitEmptyPasswords is disabled.: Status changed from passed to failed	wazuh-VMware-Virtual-Platform	1	10/03/25 9:43 PM
10	Major	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0.: Ensure sshd MaxSessions is configured.: Status changed from passed to failed	wazuh-VMware-Virtual-Platform	1	10/03/25 9:43 PM

Alert Statistics & Trends

Alert Distribution

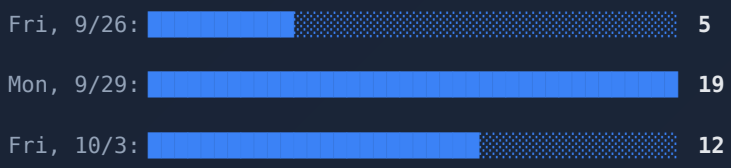
Critical	3
Major	33
Minor	0
Total Alerts	36

Alert Severity Breakdown



Critical: 8.3% | Major: 91.7% | Minor: 0%

Daily Alert Trend (Last 7 Days)



Top 5 Alert Types

sca	19
ossec	5
syslog	5
audit	4

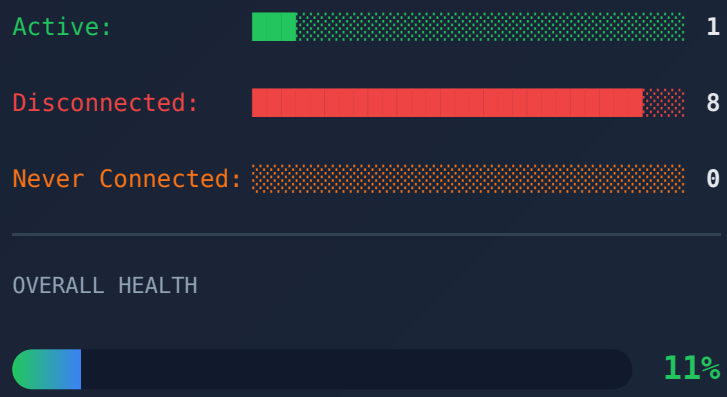
yara	3

Agent Status Overview

Agent Summary

Total Agents	9
Active	1
Disconnected	8
Never Connected	0

Agent Health Status



Agent Details

wazuh-VMware-Virtual-Platform — Active

OS: Ubuntu
IP: 127.0.0.1
Version: Wazuh v4.13.1
Last Seen: 1/1/10000, 5:29:59 AM

windows — Disconnected

OS: Microsoft Windows 11 Home Single Language
IP: 192.168.1.5
Version: Wazuh v4.13.1
Last Seen: 9/26/2025, 5:56:58 PM

Ubuntu_yara — Disconnected

OS: Ubuntu
IP: 192.168.1.29
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 1:20:48 PM

Centos_yara — Disconnected

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 2:27:33 PM

localhost.localdomain — Disconnected

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 4:43:08 PM

YARA_NEW — Disconnected

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 4:50:07 PM

Yara_Final

Disconnected

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 5:12:54 PM

Yara_New_2.0

Disconnected

OS: CentOS Stream
IP: 192.168.1.32
Version: Wazuh v4.13.1
Last Seen: 9/29/2025, 5:44:07 PM

CIS Compliance Status

Overall Compliance Score

43%

Security Configuration Assessment - Per Policy

CIS CentOS Linux 9 Benchmark (515 passed, 490 failed)	51%
CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 (127 passed, 349 failed)	27%
CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0. (96 passed, 149 failed)	39%
CIS Distribution Independent Linux Benchmark v2.0.0. (83 passed, 99 failed)	46%
CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0. (76 passed, 101 failed)	43%

Agent Compliance Scores

1. Yara_Final
103 passed, 98 failed (1 policies)
51%

2. YARA_NEW
103 passed, 98 failed (1 policies)
51%

3. localhost.localdomain
51%

4. Centos_yara
103 passed, 98 failed (1 policies)
51%

5. Yara_New_2.0
103 passed, 98 failed (1 policies)
51%

6. Sunny_Windows
83 passed, 99 failed (1 policies)
46%

7. Ubuntu_yara
76 passed, 101 failed (1 policies)
43%

8. wazuh-VMware-Virtual-Platform
96 passed, 149 failed (1 policies)
39%

9. windows
127 passed, 349 failed (1 policies)
27%

Configuration Findings Summary

Total Checks	2085
Passed	897
Failed	1188

Executive Summary

Overview

During the reporting period of September 25, 2025 - October 25, 2025, our Security Operations Center monitored and analyzed 36 security alerts across your infrastructure. The alert distribution shows 3 critical alerts, 33 major alerts, and 0 minor alerts.

Our team has been actively monitoring, triaging, and responding to security events in real-time. 9 agents are deployed across your infrastructure, with 1 currently active.

Security configuration assessment shows an overall compliance score of 43% with 1188 failed checks requiring attention.